Hacking y Pentesting con Python

Módulo 1: OSINT con Python y recolección de información activa.

eip ESCUELA INTERNACIONAL POSGRADOS

OSINT con Python y recolección de información activa.

ACTIVIDAD MODULO 1

Objetivos

- Instalar las librerías necesarias para integrar scripts en Python con servicios relacionados con técnicas tales como Shodan.
- Familiarizarse con la creación de scripts para recolectar y analizar información de sistemas objetivo.
- Aprender a utilizar Nmap desde scripts desarrollados en Python.
- Aprender a gestionar las estructuras de datos que devuelven las principales librerías orientadas a pentesting con Python.

Contenido correspondiente a modulo 1:

1. Recolección de información en Shodan.
2. Ejecución de escaneos automatizados con Nmap.
3. Ejecución de dichas rutinas desde un entorno Kali Linux.

Actividad relacionada con el módulo 1:

Kali Linux en una máquina virtual y a continuación, instala las librerías necesarias para poder ejecutar las siguientes actividades desde un script en Python

1. Leer el siguiente post sobre la vulnerabilidad CVE-2021-41773: https://www.hackplayers.com/2021/10/path-traversal-apache-2-4-49.html

2. Crear un script en Python que busque servidores web en Shodan que aparentemente son vulnerables a la vulnerabilidad de Path Transversal de Apache en su versión 2.4.49. El CVE de dicha vulnerabilidad se encuentra descrito en el siguiente enlace: https://nvd.nist.gov/vuln/detail/CVE-2021-41773
3. Partiendo de los resultados devueltos por Shodan en el script anterior, extraer las 5 primeras IPs de la lista y ejecutar un escaneo agresivo con Nmap (opción -A) contra los puertos 80 y 443. Enseñar en la terminal los detalles básicos de dicho escaneo (basta con indicar el puerto y su estado: abierto/cerrado/filtrado).